UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

| APPLICATION NO. | FILING DATE | FIRST NAMED INVENTOR | ATTORNEY DOCKET NO. | CONFIRMATION NO. |
|---|---|---|---|---|
| 09/919,240 | 07/31/2001 | Daryl Carvis Cromer | RPS9 2000 0079 | 2810 |

53493 7590 05/07/2007

LENOVO (US) IP Law
1009 Think Place
Building One, 4th Floor 4B6
Morrisville, NC 27560

| EXAMINER | |
|---|---|
| PYZOCHA, MICHAEL J | |
| **ART UNIT** | **PAPER NUMBER** |
| 2137 | |

| MAIL DATE | DELIVERY MODE |
|---|---|
| 05/07/2007 | PAPER |

**Please find below and/or attached an Office communication concerning this application or proceeding.**

The time period for reply, if any, is set in the attached communication.

| Office Action Summary | Application No. | Applicant(s) | |
|---|---|---|---|
| | 09/919,240 | CROMER ET AL. | |
| | Examiner | Art Unit | |
| | Michael Pyzocha | 2137 | |

*-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --*

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

1)☒ Responsive to communication(s) filed on *17 January 2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

4)☒ Claim(s) *1-5 and 7-28* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-5 and 7-28* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

**Application Papers**

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

**DETAILED ACTION**

1. Claims 1-5 and 7-28 are pending.

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 01/17/2007 has been entered.

***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

4. Claims 1-4, 7, 11 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hiroshi et al. (JP 2001-202167), further in view of Morikawa et al. (US 6848047), and further in view of Langford (US 6507911).

As per claim 1, Hiroshi et al. discloses a method providing security for a plurality of data records stored on a computer-readable medium within a computing system, wherein said computer readable medium additionally stores a first data structure, starting at a first location within said computer readable medium, locating data records in said plurality thereof, said method comprises an encryption subroutine executed as said computing system is being shut down and a decryption subroutine executed as said computing system is being initialized(see paragraph [0004]), said encryption subroutine includes receiving a request to shut down said computing system, reading said first data from said computer readable medium, encrypting said first data with a public key of said computing system, to produce an encrypted version of said first data that can only be decrypted with a private key of said computing system to prevent reading information stored in said data records with said computer readable medium removed from said computing system, storing said encrypted version of said first data in nonvolatile storage, starting at a second location within said nonvolatile storage(see paragraph [0017]), and said decryption subroutine includes determining that electrical power has been turned on in said computing system, reading said encrypted version of said first data from said nonvolatile storage, decrypting said

encrypted version of said first data with said private key of said computing system to form said first data structure, and writing said first data structure to said computer readable medium, starting at said first location (see paragraph [0019]).

Hiroshi et al. discloses the encryption of only the header of a file (see paragraph [0012]), but fails to explicitly disclose encrypting a data structure as opposed to the entire file.

However, Morikawa et al. teaches such encryption of a header file (see column 12 lines 19-30).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to not encrypt all of the data of Hiroshi et al.

Motivation to do so would have been to save processing power and to only allow a predetermined terminal to access the data.

The modified Hiroshi et al. and Morikawa et al. system fails to explicitly disclose, as a part of the encryption method, deleting said first data structure from said computer readable medium, and storing said encrypted version of said first data structure in nonvolatile storage, starting at a second location within said nonvolatile storage, and, as a part

of the decryption method, writing said data structure to said computer readable medium, starting at said first location.

However, Langford teaches such a replacement method (see column 4 line 63 through column 5 line 18).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use Langford's method of overwriting in the modified Hiroshi et al. and Morikawa et al. system.

Motivation to do so would have been to allow no plaintext of the original data to be present (see Langford column 5 lines 1-18).

As per claims 2-3, the modified Hiroshi et al., Morikawa et al. and Langford system discloses the second location is at the first location on the readable medium (see Langford column 4 line 63 through column 5 line 18).

As per claim 4, the modified Hiroshi et al., Morikawa et al. and Langford system discloses the nonvolatile storage is a memory structure, separate from said computer readable medium, with said computing system (see Hiroshi et al. paragraph [0020]).

As per claim 7, the modified Hiroshi et al., Morikawa et al. and Langford system discloses the encrypted version of said first data structure is equal in length to said first data

structure (see Langford column 4 line 62 through column 5 line 18).

As per claims 11-12, the modified Hiroshi et al., Morikawa et al. and Langford system discloses said method additionally comprises a configuration subroutine providing a user interface for setting and resetting a configuration bit, and said encryption subroutine is executed according to a state of said configuration bit and said encryption subroutine additionally includes setting a flag bit in non-volatile storage, and said decryption subroutine is executed only when said flag bit is set (see Morikawa et al. column 12 lines 19-30).

5. Claims 5, and 13-24 and rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Hiroshi et al., Morikawa et al. and Langford system as applied to claim 1 above, and further in view of Narad et al. (US 6157955).

As per claims 5, 13 and 19, the modified Hiroshi et al., Morikawa et al. and Langford system discloses a method providing security for a plurality of data records stored on a computer readable medium within a computing system, wherein said computer medium additionally stores a first data structure starting at a first location within said removable computer readable medium, locating data records in said plurality thereof, said method comprises an encryption subroutine executed to encrypt said

first data structure and a decryption subroutine subsequently executed to decrypt an encrypted version of said first data structure, said encryption subroutine includes reading said first data structure from said computer readable medium, encrypting said first data structure within a cryptographic processor in said computing system using an encryption key to produce an encrypted version of said first data structure, deleting said first data structure from said computer readable medium, and storing said encrypted version of said first data structure in nonvolatile storage, starting at a second location within said nonvolatile storage, and said decryption subroutine includes reading said encrypted version of said first data structure from said nonvolatile storage, decrypting said encrypted version of said first data structure within said cryptographic processor in said computing system using a decryption key generated from data stored in secure storage accessed by said cryptographic processor to form said first data structure, and writing said data structure to said computer readable medium, starting at said first location (see rejection of claim 5) with the prevention of reading records when the medium is removed from the system (see Hiroshi et al. as applied to claim 1).

The modified Hiroshi et al., Morikawa et al. and Langford system fails to disclose the use of a separate cryptographic processor.

However, Narad et al. teaches the use of a separate cryptographic processor (see column 7 lines 4-6).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use a separate cryptographic processor in the modified Hiroshi et al., Morikawa et al. and Langford system.

Motivation to do so would have been to accelerate encryption functions (see Narad et al. column 7 lines 4-6)/

Claims 14-16 and 20-22 are rejected as in claims 1, 11-12 respectively.

As per claims 17-18 and 23-24, the modified Hiroshi et al., Morikawa et al., Langford and Narad et al. system discloses a cryptographic selection subroutine providing a graphical user interlace, said cryptographic selection subroutine includes displaying a choice between encryption and decryption, displaying representations of computer readable medium in said computing system, and receiving a cryptographic selection signal indicative of whether encryption or decryption is to occur and of a chosen computer readable medium, said encryption subroutine is executed in response to receiving cryptographic selection

signal indicating encryption is to occur, with said first data structure of said chosen computer readable medium being encrypted, and said decryption subroutine is executed in response to receiving a cryptographic selection signal indicating decryption is to occur, and with said encrypted version of said first data structure of said chosen computer readable medium being decrypted wherein said encrypted version of said first data structure is stored in nonvolatile storage on said chosen computer readable medium (see Langford column 6 lines 52-67 for the GUI and the encryption/decryption and hard drives as in Hiroshi et al. applied to previous claims).

6. Claims 8-9 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Hiroshi et al., Morikawa et al. and Langford system (alone or in combination with Narad et al.) as applied to claims 1 and 19 above, and further in view of Robinson et al. (US 5544356).

As per claims 8-9 and 25, the modified Hiroshi et al., Morikawa et al. and Langford system (alone or in combination with Narad et al.) fails to disclose the computer readable medium additionally stores a second data structure, starting at a second location within said computer readable medium, describing characteristics of said first data structure, and said encryption subroutine additionally includes reading said

second data structure to determine characteristics of said first data structure wherein said first data structure is a file allocation table, and said second data structure is a boot record.

However, Robinson et al. teaches a boot record describing the file allocation table (see column 1 line 64 through column 2 line 4).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the modified Hiroshi et al., Morikawa et al. and Langford system (alone or in combination with Narad et al.) to encrypt Robinson et al.'s file allocation table.

Motivation to do so would have been that the boot record includes the number of copies of the file allocation table (see Robinson et al. column 1 line 64 through column 2 line 4).

7. Claims 8, 10 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Hiroshi et al., Morikawa et al. and Langford system (alone or in combination with Narad et al.) as applied to claims 1 and 19 above, and further in view of Starek et al. (US 6070174).

As per claims 8, 10 and 25, the modified Hiroshi et al., Morikawa et al. and Langford system (alone or in combination with Narad et al.) fails to disclose the computer readable

medium additionally stores a second data structure, starting at a second location within said computer readable medium, describing characteristics of said first data structure, and said encryption subroutine additionally includes reading said second data structure to determine characteristics of said first data structure wherein said first data structure includes an array of file records in a master file table of a NTFS file, and said second data structure includes metafile data in said master file table.

However, Starek et al. teaches such data structures (see column 10 lines 29-51).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the modified Hiroshi et al., Morikawa et al. and Langford system (alone or in combination with Narad et al.) to encrypt Starek et al.'s file array.

Motivation to do so would have been that the metafile describe the file system structure (see column 10 lines 29-51).

8. Claims 26-28 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hiroshi et al. (JP 2001-202167), further in view of Morikawa et al. (US 6848047.

As per claims 26-28, Hiroshi et al. discloses providing security for a plurality of data records stored with a first

data structure locating data records in said plurality thereof on a computer readable medium within said computing system, wherein said method comprises: encrypting said first data to form an encrypted version of said first data as said computing system is being shut down (see Hiroshi et al. paragraph [0017]), and decrypting said encrypted version of said first data as said computing system is being initialized; wherein said first data is encrypted with a public key of said computing system and decrypted with a private key of said computing system (see Hiroshi et al. paragraph [0019]); and writing said encrypted version of said first data structure to said computer readable medium after encrypting said first data structure; and reading said encrypted version of said first data structure from said computer readable medium before decrypting said encrypted version of said computer readable medium (see Hiroshi et al. paragraph [0019]).

Hiroshi et al. discloses the encryption of only the header of a file (see paragraph [0012]), but fails to explicitly disclose encrypting a data structure as opposed to the entire file.

However, Morikawa et al. teaches such encryption of a header file (see column 12 lines 19-30).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to not encrypt all of the data of Hiroshi et al.

Motivation to do so would have been to save processing power and to only allow a predetermined terminal to access the data.

***Response to Arguments***

9. Applicant's arguments with respect to claims 1-5 and 7-28 have been considered but are moot in view of the new ground(s) of rejection.

***Conclusion***

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Foster et al. (US 6853727) teaches a method of only encrypting a data structure of a file, but contains a common assignee.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Emmanuel Moise can be reached on (571) 272-3865. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJP

EMMANUEL L. MOISE
SUPERVISORY PATENT EXAMINER